	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Cookie 1	acme.com	TRUE	/	Name	Alice	FALSE	12/31/99
⋮			⋮		⋮		
Cookie n	acme.com	TRUE	/	Role	manager	FALSE	12/31/99

Figure 1: An Example of Cookies on the Web

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
IP_Cookie	acme.com	TRUE	/	IP_Cookie	129.174.100.88	FALSE	12/31/99
Pswd_Cookie	acme.com	TRUE	/	Pswd_Cookie	hashed_password	FALSE	12/31/99
KT_Cookie	acme.com	TRUE	/	Kerberos_Ticket	$\{Alice, K_{c.s}\}Ks$	FALSE	12/31/99
Sign_Cookie	acme.com	TRUE	/	Sign_Cookie	Signature_of_Alice	FALSE	12/31/99

Figure 2: Authentication Cookies

TGT = $\{S_A, Alice\}K_{KDC}$
TSK_Cookie = $\{timestamp\}S_A$, Alice, Bob
$T_{c.s}$ = $\{Alice, Kc.s\}Ks$ (ticket to Bob)
TSS_Cookie = $\{timestamp\}Kc.s$
TSS'_Cookie = $\{timestamp+1\}Kc.s$

1. Request TGT
2. TGT_Cookie = $\{TGT, S_A\}Kc$
3. TGT_Cookie = TGT
   TSK_Cookie
4. KT_Cookie =Tc.s
   KC_Cookie = $\{Kc.s, Bob\}S_A$
5. KT_Cookie =Tc.s
   TSS_Cookie
6. TSS'_Cookie

TSK_Cookie : Timestamp for the KDC
KT_Cookie : Kerberos Ticket Cookie
KC_Cookie : Kerberos Client Cookie
TSS_Cookie : Timestamp for the Server

Figure 3: Kerberos-based Authentication with cookies

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Cookie 1	acme.com	TRUE	/	Name	Alice*	FALSE	12/31/99
Cookie n	acme.com	TRUE	/	Role	manager*	FALSE	12/31/99
Pswd_Cookie	acme.com	TRUE	/	Pswd_Cookie	hashed_password	FALSE	12/31/99
Key_Cookie	acme.com	TRUE	/	Key_Cookie	encryped_key*	FALSE	12/31/99

Sealing Cookies

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Seal_Cookie	acme.com	TRUE	/	Seal_Cookie	Seal_of_Cookies**	FALSE	12/31/99

* Sensitive fields can be encrypted in the cookies.
** Seal of Cookies can be either MAC or signed message digest of cookies.

Pswd_Cookie can be replaced with one of other authentication cookies in Figure 2

Figure 4: A Set of Secure Cookies on the Web

Pswd_Cookie can be replaced with one of other authentication cookies in Figure 2
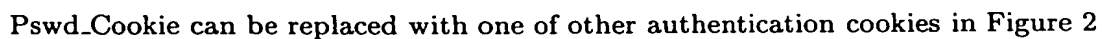
Figure 5: How to use Secure Cookies on the Web
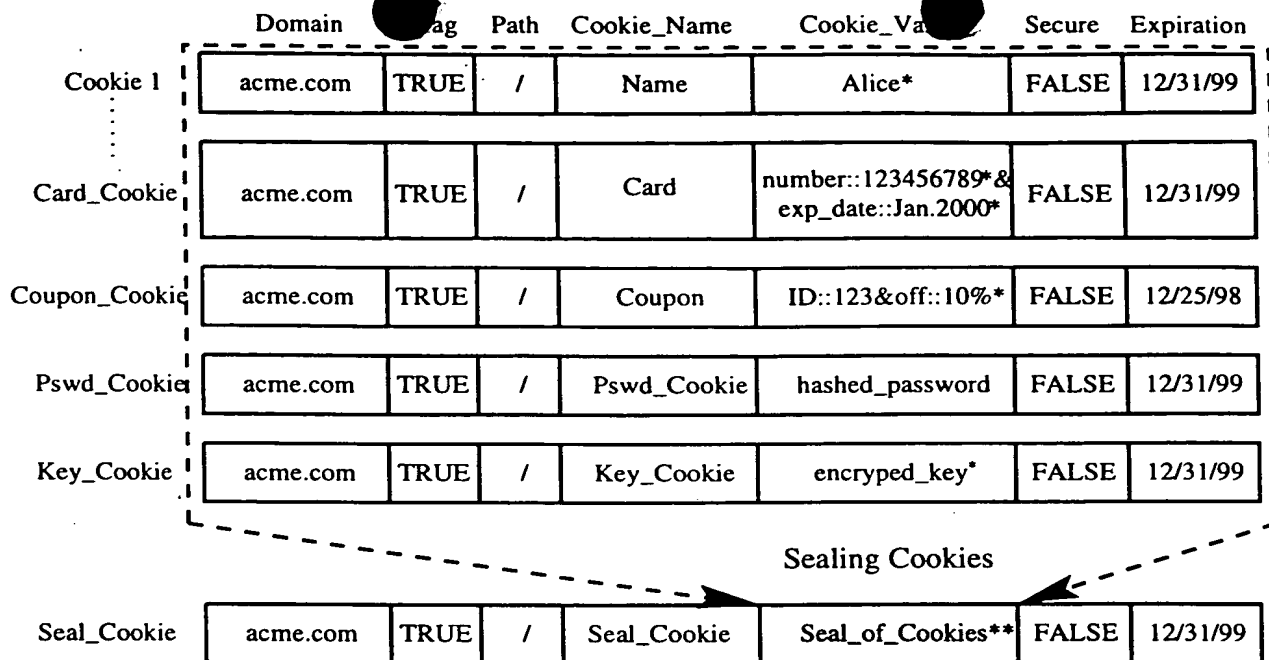
	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Cookie 1	acme.com	TRUE	/	Name	Alice*	FALSE	12/31/99
Card_Cookie	acme.com	TRUE	/	Card	number::123456789*& exp_date::Jan.2000*	FALSE	12/31/99
Coupon_Cookie	acme.com	TRUE	/	Coupon	ID::123&off::10%*	FALSE	12/25/98
Pswd_Cookie	acme.com	TRUE	/	Pswd_Cookie	hashed_password	FALSE	12/31/99
Key_Cookie	acme.com	TRUE	/	Key_Cookie	encryped_key*	FALSE	12/31/99

Sealing Cookies

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Seal_Cookie	acme.com	TRUE	/	Seal_Cookie	Seal_of_Cookies**	FALSE	12/31/99

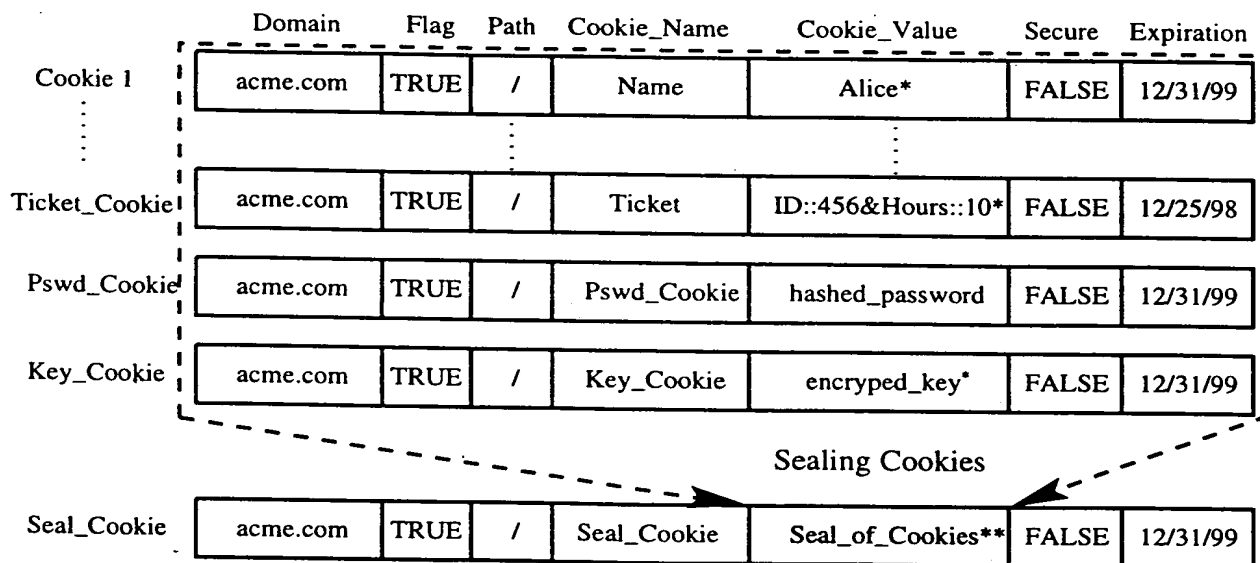* Sensitive fields can be encrypted in the cookies.

** Seal of Cookies can be either MAC or signed message digest of cookies.

Pswd_Cookie can be replaced with one of other authentication cookies in Figure 2

Figure 6: An Example of Secure Cookies for Electronic Transactions

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Cookie 1	acme.com	TRUE	/	Name	Alice*	FALSE	12/31/99
Ticket_Cookie	acme.com	TRUE	/	Ticket	ID::456&Hours::10*	FALSE	12/25/98
Pswd_Cookie	acme.com	TRUE	/	Pswd_Cookie	hashed_password	FALSE	12/31/99
Key_Cookie	acme.com	TRUE	/	Key_Cookie	encryped_key*	FALSE	12/31/99

Sealing Cookies

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Expiration
Seal_Cookie	acme.com	TRUE	/	Seal_Cookie	Seal_of_Cookies**	FALSE	12/31/99

* Sensitive fields can be encrypted in the cookies.

** Seal of Cookies can be either MAC or signed message digest of cookies.

Pswd_Cookie can be replaced with one of other authentication cookies in Figure 2
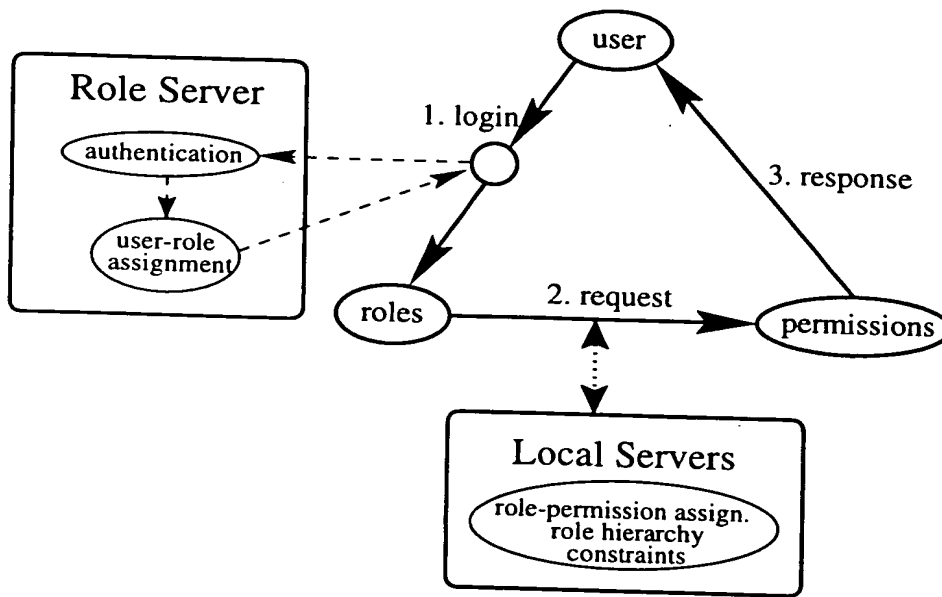
Figure 7: An Example of Secure Cookies for Pay-per-Access

Figure 8: A Schematic of RBAC on the Web